TATA 54 (NUMBER THEORY)
August 30, 2014
(SKETCHES OF) SOLUTIONS

(1) $N \equiv 7^{171} \pmod{10}$, since $47 \equiv 7 \pmod{10}$.
Now $\varphi(10) = 4$ and Euler's theorem implies that $7^4 \equiv 1 \pmod{10}$,
[This congruence also follows from $7^4 \equiv (7^2)^2 \equiv 49^2 \equiv 9^2 \equiv (-1)^2 \equiv 1 \pmod{10}$]
and therefore $7^{171} \equiv 7^3 \equiv 49 \cdot 7 \equiv$
$\equiv (-1) \cdot 7 \equiv 3 \pmod{10}$, since
$171 \equiv 3 \pmod{4}$.
ANSWER: 3

(2) A positive integer is the sum of the squares of two integers precisely when each prime number $\equiv 3 \pmod{4}$ occurs to an even power in its prime factorization.
Now $1230 = 3 \cdot 410 = 2 \cdot 5 \cdot 3 \cdot 41$
and $1233 = 3 \cdot 411 = 3^2 \cdot 137$.
ANSWER (a) NO (b) YES

(3) (a) By the law of quadratic reciprocity for the Jacobi symbol.
$$\left(\frac{35}{141}\right) = \left(\frac{141}{35}\right) = \left(\frac{1}{35}\right) = 1.$$

(3ac(d)): We have used that
$141 \equiv 1 \pmod 4$ and $141 \equiv 1 \pmod{35}$

(b) Nevertheless, there is no integer x such that $x^2 \equiv 35 \pmod{141}$. Note that $3 \mid 141$ and therefore $x^2 \equiv 35 \pmod{141} \Rightarrow x^2 \equiv 35 \pmod 3 \Rightarrow x^2 \equiv 2 \pmod 3$ and the last congruence has no solution!

ANSWER (a) 1 (b) NO

(4) $8910 = 10 \cdot 891 = 10 \cdot 9 \cdot 99 =$
$= 2 \cdot 3^4 \cdot 5 \cdot 11$

$8911 = 7 \cdot 1273 = 7 \cdot 19 \cdot 67$

Since $7-1=6$, $19-1=18$, $67-1=66$ all divide 8910, 8911 must be a Carmichael number.

[n is a Carmichael number if and only if $n = q_1 \cdots q_k$ where $q_1, \ldots, q_k$ are distinct odd primes ($k \geq 3$), such that $q_i - 1 \mid n-1$ for all i.]

(5) Since $46 = 2 \cdot 23$ for all integers a such that $47 \nmid a$, $\mathrm{ord}_{47}\, a \in \{1, 2, 23, 46\}$

(5 a ctd): $5^3 = 125 \equiv -16 \pmod{47}$

$5^4 \equiv -16 \cdot 5 \equiv -80 \pmod{47}$

$5^6 \equiv (-16)^2 \equiv 256 \equiv 21 \pmod{47}$

$5^{10} = 5^4 \cdot 5^6 \equiv -80 \cdot 21 \equiv -40 \cdot 42 \equiv$

$\equiv 7 \cdot (-5) \equiv -35 \equiv 12 \pmod{47}$

$5^{20} = (5^{10})^2 \equiv 12^2 \equiv 144 \equiv 3 \pmod{47}$

$5^{23} = 5^3 \cdot 5^{20} \equiv -16 \cdot 3 \equiv -48 \equiv -1 \pmod{47}$ Hence we must have $\operatorname{ord}_{47} 5 = 46$ and 5 is a primitive root mod 47.

(b) In (a) we noted that $5^3 \equiv -16 \pmod{47}$

So $16 \equiv -5^3 \pmod{47} \equiv 5^{23} \cdot 5^3 \pmod{47}$

$\equiv 5^{26} \pmod{47}$, and therefore

$\operatorname{ind}_5 16 = 26$.

Hence $5^{3x} \equiv 16 \pmod{47} \iff 3x \equiv 26 \pmod{46}$

$\iff 15 \cdot 3x \equiv 15 \cdot 26 \pmod{46} \iff$

$(15, 46) = 1$ $\qquad (-1)x \equiv 15 \cdot (-20) \pmod{46}$

$\iff x \equiv 15 \cdot 20 \equiv 300 \equiv 24 \pmod{46}$

ANSWER: $x = 24 + n \cdot 46,\ n = 0, 1, 2, \ldots$

6 (a) $\sigma(n) = \sigma(3^k)\sigma(5^l) = \frac{3^{k+1}-1}{3-1} \cdot \frac{5^{l+1}-1}{5-1}$

$$\frac{\sigma(n)}{2n} = \frac{(3^{k+1}-1)(5^{l+1}-1)}{2 \cdot 2 \cdot 4 \cdot 3^k 5^l} = \frac{1}{16}\left(3 - \frac{1}{3^k}\right)\left(5 - \frac{1}{5^l}\right)$$

$< \frac{15}{16} < 1$.

6 (b) $\sigma(n) = \sigma(3^k)\,\sigma(p^e) =$

$$= \frac{3^{k+1}-1}{2} \cdot \frac{p^{e+1}-1}{p-1}$$

$$\frac{\sigma(n)}{2n} = \frac{(3^{k+1}-1)(p^{e+1}-1)}{2 \cdot 2 \cdot (p-1) \cdot 3^k p^e} = \frac{\left(3 - \frac{1}{3^k}\right)\left(p - \frac{1}{p^e}\right)}{4(p-1)}$$

$$< \frac{3p}{4(p-1)} < 1, \text{ since}$$

$$\frac{3p}{4(p-1)} < 1 \iff 3p < 4(p-1) \iff$$

$p > 4$, which is true by hypothesis.

Hence $\sigma(n) < 2n$ and n is not a perfect number.